

NIT-307  
NT0503US

LIST OF INVENTOR'S NAME AND ADDRESS

Yoshinobu IKEDA, Tokyo, JAPAN.

100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2220  
2221  
2222  
2223  
2224  
2225  
2226  
2227  
2228  
2229  
2230  
2231  
2232  
2233  
2234  
2235  
2236  
2237  
2238  
2239  
2240  
2241  
2242  
2243  
2244  
2245  
2246  
2247  
2248  
2249  
2250  
2251  
2252  
2253  
2254  
2255  
2256  
2257  
2258  
2259  
2260  
2261  
2262  
2263  
2264  
2265  
2266  
2267  
2268  
2269  
2270  
2271  
2272  
2273  
2274  
2275  
2276  
2277  
2278  
2279  
2280  
2281  
2282  
2283  
2284  
2285  
2286



## INFORMATION DISTRIBUTING SYSTEM AND METHOD THEREOF

## BACKGROUND OF THE INVENTION

The present invention relates to an information  
5 processing system connected to the Internet. More specifically  
the present invention relates to a system and method for  
protecting information stored within a system from unauthorized  
tampering from inside or outside the system.

In recent years, mutually connected computer equipment  
10 is being utilized for a variety of applications due to the  
spread of the Internet. Methods such as the following have  
been implemented as a means to prevent illegal access to these  
kinds of computers. The most typical protection means is  
illustrated in FIG. 12. A system called a firewall is connected  
15 between the information processing system and the Internet.  
Services provided over the Internet can be limited by using  
the firewall to reject unauthorized access.

The computer equipment providing the service is installed  
outside the firewall as shown in FIG. 13, and in some cases  
20 protective measures are also installed on the computer  
equipment. Technology for installing a mail server external  
to the firewall in a system such as shown in FIG. 13 is disclosed  
in JP-A No. H11-266279. In a system of this kind, the user  
on the external side of the firewall can send or receive mail  
25 without using the firewall, and security within the firewall

is enhanced.

#### SUMMARY OF THE INVENTION

The protective system of the prior art relied on a system  
5 called a firewall, generally requiring high installation and  
management costs. The strength of the protective system using  
a firewall depended on the ability of the firewall to withstand  
external attack. Also, various functions had to be added to  
the information processing system according to the various  
10 services provided over the Internet. These added functions  
made the internal configuration of the firewall more complex  
and created the problems of weaker performance and new holes  
in the security.

In a configuration with the service provider device  
15 installed externally to the firewall as shown in FIG. 13, due  
to the need for protection from external attack, the  
configuration did not allow easy access to the device providing  
the service from the inner side of the firewall. The typical  
firewall can withstand an external attack but no consideration  
20 was given to unauthorized tampering from within, so the firewall  
is not effective against internal attack. Further, when  
unauthorized tampering with information has occurred in an  
information processing system of the prior art, such tampering  
is not easy to detect, causing the problem of high costs for  
25 constant monitoring to discover illegal accessing.

The proxy server of the prior art has the objectives of proxy connection to the external Internet (attempting a connection with the WWW server requested by the user on behalf of the user computer running the WWW browser software, and if successfully connected, sending that acquired data from that WWW server to the user) as well as the objective of temporary storage (along with sending data acquired from the WWW server to the user, temporarily storing that data in its own memory space to prepare for a request for that data). The proxy server of the prior art was therefore not capable of protecting the (external) service provider device during inner side Internet connections. The mirror server of the prior art had the objectives of copying the contents of the target mirror server to lighten the load on the system and network, so no special consideration was given to protecting the system. The mirror server and the proxy server of the prior art were therefore no different from the protective system of the prior art in terms of security.

The present invention therefore has the objective of providing a system capable of lowering system operating costs and easily monitoring devices providing services over the Internet for unauthorized tampering. Other objectives of the invention will become apparent from the following description.

In the present invention, a plurality of replicas (copies) of the service provider system on the inner side of the firewall,

are installed on the outer side of the firewall, and the user receives service provided only from these replicas. The service provider stores the information on the main service provider system on the inner side of the firewall. Since this system  
5 is on the inner side of the firewall, the information can be stored by various means without worrying about holes in the security.

The plurality of replicas serve to copy and rewrite the information of the main service provider system. Each replica  
10 periodically compares information contents with the information held by the other replicas to check if unauthorized tampering has occurred. When a discrepancy (difference) is detected among information held by the replicas, the main data  
15 from the service provider system on the inner side of the firewall is copied onto the replica, and a check made to determine if unauthorized tampering is present on the replica, and corrections can be made per the source information and a report made to the administrator.

A digital signature can be added to the information copied  
20 onto the replica. When using this function, the replica checks whether or not the digital signature for information transmitted to the user is valid, and when found to be valid sends the information, and when found to be invalid contacts the administrator (after the replica contacts the WWW server  
25 with the information that the signature is invalid, the WWW

server contacts the administrator by mail or SNMP message, etc.). In the above configuration, persons without the right (access permission) to add the required digital signature can be rendered unable to open or change (tamper) with the information.

By interchanging the servers performing the services the plurality of replicas can appear as the same device as seen from the Internet. In the above configuration, devices can be separated into devices illegally connected internally and those that are legally connected and these devices can be mutually compared. The load on the replicas providing the service can also be dispersed, and a drop in speed can be prevented.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a concept system block diagram showing an embodiment of the present invention.

FIG. 2 is flow chart showing the operation in the firewall.

FIG. 3 is a drawing showing a typical structure of a domain name.

FIG. 4 is a system block diagram with a hidden firewall and improved protection compared to FIG. 1.

FIG. 5 is a system block diagram utilizing a switch and having improved protection and an improved load dispersing function compared to FIG. 4.

FIG. 6 is a block diagram showing when mounted with the equipment of the system in FIG. 5.

FIG. 7A and 7B are drawings showing the instant rewrite function.

5 FIG. 8 is a drawing showing the comparison check.

FIG. 9 is a flow chart showing the information transmit control utilized for the digital signature.

FIG. 10 is a drawing showing the transmit control for rating the digital signature.

10 FIG. 11A and 11B are flow charts showing the information transmit control utilized for a plurality of digital signatures.

FIG. 12 is a block diagram of the system of the prior art.

15 FIG. 13 is a block diagram showing another example of the prior art.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A block diagram of the embodiment of the system for  
20 providing a WWW service in the present invention is shown in FIG. 1. A local area network (LAN) is connected as the intra-company network to the Internet 1 by way of a firewall 2 in FIG. 1. A WWW service such as a WWW server 3 for providing web page(s) for example and a storage information system 4  
25 utilized for creating information for storage in the WWW server



are connected in the inter-company network. The firewall 2 is here comprised of a communications section for carrying out communications with the Internet side and replica 8 side, and a communications section for carrying out communications with the intra-company network side. The firewall 2 also has a control section to control access request to the intra-company network from the Internet side. Though not shown in the drawing, the firewall 2 has a memory section for storing programs involving processing by the control section.

The storage information maker system 4 on the intra-company network side runs on information processing equipment such as the PC. The operator stores information from the storage information maker system 4 into the memory of the WWW server 3. Besides communicating with the PC4 by way of the LAN, the WWW server 3 has a communications section for data transfer with the replica 8 by way of the firewall 2. Based on the signal received via the communications section, the control section processes information in the memory section, processing information stored in the memory section such as from the PC, and sending information in response to a transmit request from the firewall 2. Programs used by the control section to run this processing are stored in the memory section. Any generally used network transfer procedure can be utilized at this time because of protection by the firewall 2. The WWW server 3 can be selected for example as a file server, and

file sharing performed between the WWW server 3 and the storage information system 4.

The replica 8 has a communications section for sending information and receiving information from the WWW server 3 via the firewall 2 and for sending and receiving information from the Internet. The replica 8 also contains a memory section for copying all the contents of the WWW server 3. The control section also performs storage in the memory section, CRC calculation and comparison processing. The processing by the control section is achieved by programs stored in the memory section. The copying of all contents of the WWW server 3 is a basic function however the copy quantity and the location for copying can also be set. In other words, when the contents on the server are comprised of a plurality of directories and files, from where to where the file and directories will be copied can be specified. Limits can also be specified on the number and size of files targeted for copying. Control can be achieved for example, by placing limits on the number and overall size of file for copying onto each directory, and by limits such as on the size of files for copying. The item for copying can also be automatically selected and actively changed according to factors such as capacity and frequency of access, etc.

A plurality of replicas 8 constituting caches of the WWW server 3 are connected to the outer side of the firewall 2.

In FIG. 1, there are only four replicas 8 units and one WWW server 3 unit as seen from the Internet 1. However, more units than shown here may be connected during actual use. Conversely, the number of replicas 8 units may be more than one. Further, one device may be connected to a plurality of units. The replicas 8 may further be connected in multiple stages. These replicas 8 may also be in other locations on the Internet, and the disposition structure of replicas 8 may be utilized to disperse the load on the network. A domain name server 9 is connected to the Internet, and this domain name server 9 changes the domain name to an IP address.

The connection processing between the replica 8, firewall 2 and the WWW server 3 is next described while referring to FIG. 2. The replica 8 carries out communications with the WWW server 3 via the firewall 2, regardless of the connection processing. In this case, the firewall 2 only opens the HTTP port to an external network. If a communication from an external network is through a port other than an HTTP port, (step 201 No.) then the firewall 2 cuts off this communication. If the communication from an external network is for an HTTP port (step 201 Yes) then the firewall identifies the transmission source from the information within the packet header, and determines whether or not it is a connection request from replica 8 (step 202). The connection is permitted if the packet transmission source is the replica 8 located in an external

network but is cut off the transmission if the transmission source is another device. If the device for the connection request from an HTTP (port) is the replica 8, then the firewall 2 permits a connection to the replica 8.

5           The replica 8 having received a reply from the firewall 2 permitting connection, creates the command (step 203) and sends the request for processing to the WWW server 3. At the firewall 2 located between the WWW server 3, the command from the replica 8 is received and a syntax check of the command made (step 204). If an error is determined to be present in the syntax, then the communication is cut off. If the results of the check show that the syntax is correct, then the firewall 2 makes a connection request per the HTTP to the WWW server 3. The WWW server 3 identifies the transmission source of the connection request (step 205) and if the source is the permitted device, then a response is returned permitting correction, but if not then the permitted device then the transmission is cutoff. The firewall 2 having received permission for connection, sends the commands transmitted from the replica 8, to the WWW server 3. The WWW server 3 that received the command from the firewall 2, creates data according to the processing requested by the command (1006). Upon receiving this data, the firewall 2 sends this data to the replica 8 and, accepts further new commands per the replica 8. When the replica 8 then makes a processing request to the WWW server

3, the processing performed after creating the commands per replica 8 is repeated (1007 No.). If there are no requests to the WWW server 3, then the replica 8 sends a request to the firewall 2 to cutoff the communication. The firewall 2 makes the same request to WWW server 3 to cutoff the communication, so that the communication between the replica 8, the firewall 2 and the WWW server 3 is then cutoff and the processing ends.

As described above, the firewall accepts only connection requests from the replica that utilized the HTTP so that restrictions can be placed on access even if not using an expensive, commercial firewall system. An HTTP proxy server for example can be built inexpensively by utilizing free software and can also be utilized as the firewall. Alternatively, the firewall and WWW server previously installed by the customer can be utilized as is. In this case, the customer installs a new replica 8, makes additional settings on the WWW server (adding of replica copy, rewrite functions) to form the WWW server 3. In this configuration, the replica 8 forms the copy (or duplicate) of the WWW server 3. In either case, a replica 8 utilizing only a general HTTP connection becomes the duplicate (or copy) of the WWW server 3, and the contents of the WWW server 3 cannot be rewritten from the replica 8. Unauthorized access to the WWW server 3 can in this way be restricted by the replica 8 and a firewall with a simple structure. The protection can be even further enhanced by a configuration

described later on, when a system has two or more of the replica  
8. In this embodiment, the WWW server was used as an example  
so that access was restricted to the HTTP port, needless to  
say however, restrictions can be implemented by the protocol  
5 matching each respective server. Furthermore, a protocol such  
as HTTPS capable of implementing the same write-restrictions  
as HTTP may be used rather than the HTTP port.

The configuration for connecting with the user terminal  
by way of the replica 8 and the Internet 1 is described next.  
10 The replica 8 only allows communication and connection by way  
of a specified port with the user terminal not shown in the  
drawing on the Internet 1. No ports are used at this time other  
than the port having this connection and the user terminal  
isset so it cannot make a connection. In other words, connections  
15 with the Internet are controlled by utilizing the domain name  
server 9. The domain name server 9 can change the stored entry  
at any time, and disperse access so as not to be concentrated  
in the same replica. The dispersion method is shown in FIG.  
3. In FIG. 3, the user terminal, makes a connection request  
20 to the WWW server having the domain name of www.japan.co.jp.  
The domain name server 9 sends back randomly or by the round  
robin method, one of the IP addresses (1) through (4) assigned  
to the replica constituting the copy of this WWW server. The  
user terminal makes a connection with the IP address returned  
25 by this domain name server, so that user access is dispersed

among the four replicas shown in FIG. 3.

FIG. 1 showed a configuration where the replica 8 was directly connected to the Internet 1, however as shown in FIG. 4, a network different from the Internet 1 may be contrived and a connection made to the replica 8 on this network. As shown in FIG. 5, the communication path can be switched to the replica 8 by using a switch 10. The replica 8 and the firewall 2 can be connected via a network separate from the Internet 1, and by this network dispersion to the firewall 2 from the Internet 1, the system protection can be increased even further. When configured in this way, the domain name server 9 and the switch 10 can function as a load dispersing device.

The replicas 8 and the switch 10 can comprise a device consisting of a WWW security device 11 as shown in FIG. 6. In this configuration, the WWW security device 11 can be directly connected to the WWW server 3 by utilizing a typical means exterior to the network such as a dedicated cable, and the firewall 2 eliminated while still maintaining protection. In other words, even without the firewall 2, the WWW security device 11 can provide protective functions such as preventing unauthorized access from the Internet. The WWW security device 11 uses the switch 1 to disperse connection requests from the Internet 1 and distributes them to a plurality of replicas 8. A plurality of these replica 8 units may be formed in a logical structure, to allot connection requests using the

domain name server 9 such as described in FIG. 1 and FIG. 3 without using the switch 10.

The communication flow with the replica 8 and the user terminal on the Internet 1 is next described while referring to FIG. 7. A drawing showing the distribution of information by the replica 8 as requested by the user terminal is shown in FIG. 7A.

The user terminal utilizes the GET command to request the /foo/index. html file from the replica 8, however the WWW server 3 is not accessed when the replica 8 holds a copy of this file (step 701, have file). When an digital signature described later on has been added to the file the replica 8 possesses, then a check is made of that digital signature (step 703). If the digital signature is correct (step 703), then the /foo/index. html file is sent to the user. If the digital signature is incorrect (step 703 NG) then an error is reported to the WWW server 3, an error report is issued to the user stating that such a file does not exist. The check of the digital signature is optional, and if the digital signature is not used then this processing is not performed and the file is sent to the user terminal.

When the replica 8 does not possess the /foo/index. html file (step 701, no file), after establishing a connection between the replica 8 and WWW server 3 through the processing shown in FIG. 2, then a command is sent to the WWW server 3



requesting the sending of the /foo/index. html file (now copy) .  
When the WWW server 3 possesses a copy of the file (step 702,  
have file), the WWW server 3 sends that file to the replica  
8, and the replica 8 makes a check if an digital signature  
5 has been added to the file that was sent, and sends that file  
to the user. When the WWW server 3 does not possess the file  
(step 702, no file) then an error is reported to the replica  
8 as well as the user terminal from the WWW server 3.

In the above processing, the replica 8 receives a  
10 connection request on a specified port from a user terminal  
on the Internet 1, and sends a copy of the WWW server 3  
information to the user terminal. When the page with the user  
request for the new copy of the file on WWW server 3 is not  
present on the replica 8, then that information is acquired  
15 from the WWW server 3. However, the processing (rewrite) to  
show the latest information held by the WWW server 3, in the  
information held in the replica 8, can be performed by means  
of results a comparison check of the replica 8 and the WWW  
server 3.

20 The processing for carrying out the compare check  
beforehand and rewriting is shown in FIG. 7B. The replica 8  
first of all, makes a connection to the WWW server 3 or the  
cascade-connected host replica 8 (step S704). A CRC (cyclic  
redundancy check) error check code computation is then made  
25 of the applicable information (step 705). The WWW server 3

determines whether or not the requested file is present or not (step 702), and if not present (step 702, no file) sends error information to the replica 8. The replica 8 receives this and deletes the applicable file (907). If the applicable file is present (step 706, have file), then the CRC (cyclic redundancy check) error check code is calculated in the same way, and written (step 708). A rewrite date is added to this and sent to the replica 8. The CRC found by calculation and the CRC sent from the WWW server are then compared in the replica 8, to check if they match (step 709). If they match it indicates there was no rewriting of information and the replica 8 information is not rewritten (step 710). If they do not match, then the replica 8 makes a file transfer request to the WWW server and this file is saved (step 711). During this processing, communication with the user over the Internet is cutoff, and only implemented between the replica 8 and the WWW server 3.

The process for instant rewrite is shown in FIG. 7C. Instant rewrite is the rewriting (or updating) of a file on replica 8 immediately after the matching file on the WWW server 3 was rewritten. In instant rewrite, the replica 8 issues a request for rewritten information with the GET command (step 712). The WWW server 8 retains this request until rewritten information occurs, and then returns a reply with the rewritten information at the time the rewrite occurs. The rewriting of the replica 8 can in this way be performed immediately after

the rewriting of the WWW server 3.

The configuration for preventing file tampering through unauthorized access to the replica 8 is described next. Comparison checks are made at periodic intervals as explained  
 5 next between the WWW server 3 on the internal intra-company network and the mutual replicas 8, as protective measures to prevent unauthorized access or tampering from user terminals on the Internet 1 with the plurality of replicas 8 installed on an external network. These comparison checks detect  
 10 unauthorized tampering, and maintain the credibility of information held and transmitted by the replica 8.

The comparison check processing performed between the replica 8 is next described while referring to FIG. 8, for a configuration having two or more replica 8. The comparison  
 15 check processing of the /foo/index.html file held by one replica 8 unit (device A) is shown in FIG. 8. First of all, the comparison check starts by the device A using the HTTP protocol "HEAD /foo/index.html" command to make a request to the device B for sending attribute information for the /foo/index.html  
 20 file held by device B (step 801). When the device B receives the request from the device A to transmit attribute information for the /foo/index.html file, a check is made for that matching file (step 802). When the file whose transmit was requested is present, a CRC calculation of that matching file is made  
 25 (step 803), and the calculated CRC is sent to device A along

with a rewritten date. The device A on the other hand, also makes a CRC calculation of the matching file (step 804), and whether or not the CRC sent from device B and the CRC calculated by device A are a match is determined (step 805). If they match  
 5 each other, then the check is terminated since there was no illegal tampering (step 806). If they are not a match, then the device A file is determined to be incorrect due to a reason such as tampering, and the file acquired from the WWW server 3 is stored in the device A (step 810).

10 When the file that received the HEAD command from device A is not held in device B (step 802, no file), then the device B makes a connection to the WWW server 3 with the GET command and a file transmit request is made before the device B returns the HEAD command reply to the device A. If the matching file  
 15 is present in the WWW server 3 (step 807 have file), then that matching file is acquired and stored (step 808), and the CRC calculated in the same way (step 809). The calculated CRC is compared with the CRC of device A, and if the CRC match each other then the check is terminated (step 806). If they do not  
 20 match, then the file of device A is determined to be incorrect due to reasons such as unauthorized tampering, and the file acquired from the WWW server 3 is stored in the device A (step 810).

When the WWW server 3 does not have the file whose transmit  
 25 was requested, the device B decides that the file was deleted

from the WWW server 3, or was a file added to the device A over the Internet by an intruder on the network. As a reply to the HEAD command in device A, the device B sends back a delete command for the matching file and informs the WWW server 3 that a delete command has been issued in a HEAD command added with a new attribute. Alternatively, rather than deleting the file, it can be temporarily stored in a separate memory area, and stored in a designated memory region of the WWW server 3 with the POST command. In that case, the evidence of unauthorized access is left intact. These responses can all utilize encryption, and can also safely send deletion information to remote replicas on a network. Comparison checks were implemented as described above, however when implemented by custom procedures between the replica 8 and the WWW server 3, the check is not limited to the HEAD, GET, POST command specifications, and there is a greater degree of freedom in the design.

In this way, the same comparison check can be performed on other files as required by replica 8. The comparison check can be performed not only between the mutual replicas 8, but also between the replica 8 and the WWW server 3. This processing is not limited to configurations having one or more replicas 8, but can also be applied to cases where there is just one replica 8. When making a comparison check between the WWW server 3 and the other check target, the file might possibly have

been rewritten in the WWW server 3 so a rewrite check of information is also simultaneously performed (FIG. 7B) to find if the information held in the replica 8 has the newest contents.

A configuration to add new attributes to the HEAD command  
 5 (expand functions so as to also return a check code in addition to a function for returning the file data and size, etc.) and obtain a file check code (check-sums and CRC code, etc.) may also be used. The attribute information held by other devices or WWW servers and acquired with the HEAD command in this way  
 10 can be compared using these check codes so that the data to be sent and received can be non-reversibly encrypted with hash marks, etc.

The previously mentioned digital signature is explained next. The information for storage in the WWW server 3, can  
 15 be applied with a digital signature by means of signature generating procedures during storage of the data. The process flow when using the digital signature is shown in FIG. 9. The file requested with the GET command is prepared in the replica 8 (step 901). Next, a check is made for a digital signature  
 20 (step 902), and if there is no digital signature, it is determined this file cannot be sent to the user, and an Error, No-file reply is sent to the user. When a digital signature is present, this signature is evaluated (step 903), and approved or rejected for distribution to the applicable user (step 904). Data is  
 25 sent to user for whom sending was approved, or an Error, No-file

reply is sent to the user when not approved.

Though not shown in the drawings, when the signature within the distribution information is not a genuine signature, the replica 8 recopies the information held by the WWW server 3, and that signature can also be checked. Further, when the recopied information is also not genuine, a message is sent to the user reporting an error. A configuration may also be used that reports false signatures to the administrator at any stage.

The distribution information can be divided into groups as shown in FIG. 10 by utilizing the digital signatures in a configuration to control the distribution destination. As an example, the configuration in FIG. 10 shows four types of digital signatures A, B, C, D for the information. The information 1 here is added with all four types of digital signatures. This information 1 is identified by these four digital signatures as information distributed outside the company and within the company including affiliated companies. The information 2 is information added with the three types of digital signatures B, C, D. The information 2 is identified as a range of distribution information from inside the company (intra-company) and affiliated companies. The distribution range of the information from here onwards can be set according to the type of digital signature as information 3, information 4, and as information 5.

The process for dividing the distribution information into groups is described next while referring to FIG. 11. In the example, this is division into groups consisting of User A outside the company, User B in another section inside the company, and User C in the same section within the company. FIG. 11A shows the IP addresses for users A, B and C.

A detailed description of the processing is explained while referring to FIG. 11B. The replica 8 or WWW server 3 that received the data distribution request (step 1101) identifies whether the user's IP address is from within the company or outside the company (step 1102). When the user's IP address is within the company (intra-company), it is further identified to find whether or not it is the same section (step 1103). If the IP address is from the same section (user C), then the information is distributed without checking the digital signatures (step 1104). If the user IP address is from another section (user B), then along with preparing the file (step 1105), a check (step 1106) is made to determine if the digital signature added to the information for distribution is a type whose distribution to other sections is allowed. If allowed, then the information is distributed. When the user's IP address is outside the company (user A), then along with preparing the file (step 1108), a check is made to (step 1109) to determine if the digital signature added to the information for distribution is a type whose information distribution to



outside the company is allowed. If allowed, then the information is distributed, and if other than the allowed type then an error is reported to the user and the information is not distributed.

5           The above methods for utilizing the digital signature, are effective when the WWW server 3 has been grouped per application such as for inside the company and for outside the company. In other words, the distribution destination can be found by the presence (or lack) of a digital signature and differences in the digital signature. Information without a digital signature for example, is not copied onto the replica 8 or even if copied, is not distributed, so that access is only possible from a location with direct access to the WWW server 3. By therefore grouping information for outside the company by using digital signatures, and information for inside the company without using digital signatures, the distribution information can be categorized into outside company/inside company groups. In rating by means of digital signatures, control can be achieved such as for (information) distribution only to specified customers, by information recorded along with the signature.

          The replica 8 is essentially a device for making copies of information distributed by the WWW server 8, and once the copy source settings are made there is no need for operation by an operator provided no large changes occur. The copy source

settings indicate the copy policy such as to what extent to copy what server, whether or not to use a check code, whether or not to use a digital signature or code number, and whether or not to perform instant rewrite. The information allowed to pass through the firewall 2 is an accumulation of attribute information for the transmit source, etc. The attribute information accumulated in the firewall 2 can be collected in the WWW server 3. Therefore, just as with the replica 8, there is no need for the operator to manipulate the firewall 2. Since a human operator is therefore not required in operation between the replica 8 and the firewall 2, the replica 8 and the firewall 2 can be installed in rooms physically separated from each other and locked by an actual physical key. In this way, a person within the system not having the actual key, can be prevented from unauthorized intrusion and access to the system, and from disclosing or tampering with information.

There is no need to connect the replica 8 and WWW server 3 by ordinary network procedures. Therefore, if the number of communications devices on the WWW server 3 side are increased and connection made by in-house (custom) communication procedures then a firewall 2 is not needed because no Internet protocol is used. This can help lower overall system costs and prevent unauthorized system intrusion or system breakdowns from occurring due to security defects in the firewall 2. The connection for these custom procedures, does not require a

device 11 as shown in FIG. 6, and may also be implemented with a configuration as shown in FIG. 4 and FIG. 5. A firewall 2 may also be internally installed when the device 11 does not use custom procedures in communications between the replica 8 and the WWW server 3. The device 11 may also incorporate internal options of other network devices such as routers, and the device 11 may also be installed in the WWW server 3. When the system of the present invention is installed with devices such as described above, the advantage of a simpler more convenient system configuration and management is obtained.

The embodiment of the present invention was described as above, however, if multiple stages of the replica 8 are connected, and the latter stages of the replica 8 only connected to receive from the prestage, then the protective functions can be further enhanced. In that case, the replica 8 forming the pre-stage may be in another location on the Internet 1, and if installed at a location near a network with many users, then the overall network load can be lightened.

In the information transmission system of the present invention functioning on the Internet, information storage is simple, the load is reduced, and the detection of tampering and storage of unauthorized information is simple so that even if tampering occurs, the source information is easily corrected, therefore rendering the effect that great improvements can

be made in the trouble and costs involved in system structure and management.

0307254 101601